TAMPER-PROOF ENCLOSURE FOR A CIRCUIT CARD

Background of the Invention

The present invention is directed to a tamper-proof card enclosure, and more particularly to a tamper-proof card enclosure for use with a high speed communication card.

Many activities require secure communications. Diplomatic missions and military forces, for example, frequently find it necessary to communicate via messages that cannot reveal secret information if they are intercepted. Powerful encryption algorithms have been developed for converting uncoded messages into coded messages that can be transmitted securely since they can only be decoded by the intended recipient.

Financial institutions such as banks must also have access to reliable and secure communication channels to other financial institutions. The reason is that a breach in security might lead to substantial financial losses.

An encryption/decryption system may be implemented on a communications card that is included in equipment connected to a communications network. Such a communications card is an enticing target for malefactors since it may contain codes or keys to decrypt intercepted messages or to encode fraudulent messages. It is known that a communication card may be mounted in a metal enclosure which is then wrapped in a security mesh, and impregnated with polyurethane resin. A security mesh is a web or sheet of an insulating material with circuit elements such as closely spaced conductive lines fabricated on it. The circuit elements are disrupted if the mesh is torn, and this disruption

can be sensed in order to generate an alarm signal. The alarm signal may be conveyed to a monitor in order to reveal an attack on the integrity of the communications card. The alarm signal may also trigger an erasure of encryption/decryption keys stored on the communications card.

Security mesh is commercially available from W.L. Gore & Associates, Inc., having an office at 555 Papermill Road, Newark, Delaware 19711 (USA). A security mesh is also disclosed in U.S. patent 6,686,539 to Farquhar et al. The Farquhar et al patent is assigned to the Assignee of the present invention and is incorporated herein by reference.

Figure 1 is a block diagram schematically illustrating communication between two financial institutions. A financial institution 10 such as a first bank has a number of items of electrical equipment that are connected to a control unit 12. Only two items of electrical equipment are shown in the drawing (items 14 and 16), but more are typically present. These items of electrical equipment may include automatic teller machines, terminals for operation by tellers, loan offices, and other employees of the bank, information storage units, and so on. The control unit 12 includes a communication card that is connected to a communications network 20. The communications card 18 permits the control unit 12 to communicate with a similar communication card (not illustrated) in a financial institution 22, such as a second bank. The control unit 12 includes an alarm unit 24 that detects whether a security mesh (not illustrated in Figure 1) around the communications card 18 has been breached.

Summary of the Invention

It is an object of the present invention to provide a tamper-proof card enclosure with enhanced reliability at elevated temperatures.

Another object is to protect a security mesh around an enclosure that contains a card from damage due to elevated temperatures within the enclosure.

A further object is to provide a stopper member for an opening in an enclosure that is wrapped with a security mesh.

These and other objects that will become apparent from the ensuing detailed description can be attained by providing an enclosure in which a card is mounted, the enclosure having a wall with an opening in it. The card includes a printed circuit board and at least one electrical component that is mounted on it. A cup member is attached to the wall of the enclosure at the opening, the cup member having a passage. A bus is connected to conductors on the printed circuit board and passes through the passage in the cup member and through the opening in the wall. A security mesh is wrapped around the enclosure, and a portion for the security mesh covers the opening in the wall. Resin is disposed in the cup member and coats the security mesh.

In accordance with another aspect of the invention, a bus is threaded through an opening in a wall of an enclosure and through a passage in a cup member that is attached to the wall at the opening. The bus is connected to the printed circuit board, which is mounted in the enclosure. The enclosure is wrapped with a security mesh. The cup member is filled with a liquid resin, and liquid resin is also coated onto the security mesh. The resin is then cured.

Brief Description of the Drawings

Figure 1 is a block diagram schematically illustrating an example of communication between two financial institutions.

Figure 2 is a cross-sectional view of a prior art tamper-proof enclosure for a communications card; and

Figure 3 is a cross-sectional view of a tamper-proof enclosure for a communications card in accordance with the present invention.

Description of the Preferred Embodiment

The present invention arose from the discovery of a failure mode during testing of a new product by the Assignee of the present invention, and the invention of a technique for avoiding this failure mode. The new product is shown in Figure 2.

In Figure 2, an enclosure is formed by a bottom metal shell 26 and a top metal shell 28. The outer faces of the shells 26 and 28 are provided with dimples 30. The communications card 32 rests on the dimples 30 on the bottom shell 26. The communications card 32 includes a printed circuit board 34 with integrated circuits 36, and possibly additional circuit elements (not shown) that are electrically connected to conductors (not shown) fabricated on the printed circuit board.

Hollow spacers 38 are placed below the dimples 30 of the top shell 28. Rivets 40 extend through openings in the dimples 30 of the top shell 26, through the hollow spacers 38, through openings in the printed circuit board 34, and though openings in the dimples 30 of the bottom shell 26 in order to secure the communications card 32 inside the enclosure formed by the metal shells 26 and 28.

With continuing reference to Figure 2, a security mesh 42 is wrapped around the top, bottom, and four sides of the enclosure formed by the shells 26 and 28. The top shell 28 has an opening 44 through which a bus 46 extends. One end of the bus is connected to conductors (not shown) on the printed circuit board 34, and the other end is connected to conductors (not shown) on a printed circuit board 48. As it passes through the opening 44, the bus 46 extends between an inner edge region 49 of the security mesh 42 and an overlapping outer edge region 50 of the mesh 42. A group of wires 52 connect the security mesh 42 to conductors on the printed circuit board 34. Circuitry on the printed circuit board 34 is responsive to a break in the security mesh 42, in which case an alarm signal is emitted on the bus 46 and also encryption/decryption keys stored on the communications card 18 are erased.

Liquid polyurethane resin is slathered on the security mesh 42 and cured. Before it is cured, some of the resin may drip through the opening 44, and this is illustrated at 54. This is incidental, and neither improves nor hinders performance. A copper enclosure 56 is then filled with liquid polyurethane resin and the assembly is suspended in it. After the resin is cured, the communications card, enclosure, and security mesh are embedded in a polyurethane block 58, as shown.

The enclosure 56 is mounted on the printed circuit board 48. This can be accomplished by legs 60 that extend through slots in the PCB 48 and terminate in flanges 62 that are then bent out of alignment with the slots.

The bus 46 is connected, by way of the printed circuit board 48, to connectors 64 along one edge of the PCB 48.

A failure mode of the arrangement shown in Figure 2 was discovered by the inventor during the heat-cycle testing of the arrangement shown in Figure 2. In such testing, the arrangement was subjected to heating and cooling cycles, with the heating cycles increasing the temperature to 85°C. It was found that the heating increased the air pressure within the enclosure to the extent that stress on the security mesh 42 at the opening 44 was sometimes sufficient to break the security mesh. Furthermore, the polyurethane body 58 softened at high temperature, and the air pressure within the enclosure was sometimes sufficient to lift the outer edge region 50 of the security mesh and permit heated air to accumulate above the top shell 28. This accumulation of air, in turn, could cause the back wall of the enclosure 56 to bow outward.

The solution to these problems that was devised by the inventor has two aspects. First, as shown in Figure 3, polyamide resin is used to bathe the security mesh and form the body in which the enclosure is embedded. This provides a polyamide block 58' in lieu of the polyurethane block 58 shown in Figure 2. Polyamide is stiffer than polyurethane at elevated temperatures, and this decreases the proclivity of the outer edge region 50 to delaminate. Secondly, a sealing mechanism is provided at the opening 44. In Figure 3, the sealing mechanism consists of a shallow cup 64 that is connected (as by soldering) to the top metal shell 28 just below the opening 44. At its bottom, the cup 64 has a slot for passage of the bus 46 and the wires 52. The liquid polyamide resin is spread onto the security mesh 42 wrapped around the enclosure formed by the shells 26 and 28, and resin is introduced into the cup so as to fill the cup. As a result, a plastic plug that seals the opening 44 is formed. This further reduces the forces tending to delaminate the outer edge region 50 and reduces the stress on the security mesh 42 above the opening 44.

While the above explanation of the preferred embodiment of this invention has used a communications card as an example, it ill be apparent that the invention may be used with other types of cards as well.

It will be understood that the above description of the present invention is susceptible to various modifications, changes, and adaptations, and the same are intended to be comprehended within the meaning and range of equivalents of the appended claims.